

Seven Tips For Protecting Data on a Laptop

Is it really the fault of a virus protection program, or an insecure hotspot, if laptop users lose data? A recent Gartner study shows that 86 percent of all security events in wireless networks are caused by the mobile devices -- not by insecure data transfer. Utimaco Safeware, Foxboro, Mass., a mobile security specialist, offers seven simple measures for securing a notebook computer.

Tip 1: More discipline when on the move: The only protection against being careless is more care and discipline --- but that is difficult when under a time pressure. Airline passengers lost more than 5,000 mobile devices at airports in Germany, Austria and Switzerland a survey conducted by Utimaco Safeware AG among the Lost and Found offices at the ten largest airports in the region revealed. Particularly at airports with a large number of short-distance routes that are primarily used by business travelers, several dozen mobile devices are turned in daily -- on heavily traveled days, as many as a hundred. It might sound obvious, but if you travel with a notebook, you should always make sure that you really have the notebook case, including all its contents, over your shoulder before you leave the plane, taxi or train.

Tip 2: Make passwords more difficult to crack: If the worst happens, and your computer is stolen or lost, there is still hope that your personal data is not all accessible, if the password is difficult enough to crack. A mixture of characters, numbers and letters is considered the most secure -- but only if passwords and keys are not stored on the hard disk. For this reason it is better if the computer prompts for a password before booting, which electronic security solutions can enable.

Tip 3: Use hardware to supplement password protection: Analysts working for the Meta Group have confirmed what IT managers already know: passwords alone do not provide optimum protection for data. The alternatives have been available, and in use, for years: special smartcards or tokens -- which look just like a USB stick -- store key information that is used in combination with a user password to unlock the computer. Only someone who has the token and knows the password can access the system and the data saved on it. Alternatively, the user's biometric data can be stored on a smart card. For authentication, the user's fingerprint is checked directly on the card, instead of the password.

Tip 4: Secure hibernation mode: Set up the system to prompt for the password again when the notebook switches back from the screen saver or from hibernation mode to normal working mode.

Tip 5: Set up an electronic safe: A basic principle is you should never save valuable information without protecting it electronically: important papers are kept in safes. The electronic pendant is a "virtual" disk drive that securely encrypts and stores all its contents. You can easily set up an electronic safe of this kind on local hard disks and network directories, on the PDA, and also on mobile devices such as USB sticks and smart cards, CD-ROMs and DVDs.

Tip 6: Implement automatic encryption: Data transparent encryption is a big help when using electronic safes. It runs automatically in the background, without being noticed, so the user does not even have to think about storing data securely.

Tip 7: Restrict plug and play: Plug and Play is convenient, but can sometimes be dangerous: if someone connects a USB stick, MP3 player or external hard disk drive to a notebook, it is recognized automatically -- and it is then easy to start exporting data. The alternative is to lock the computer for all memory media apart from the company's own memory sticks which cannot be used to run or read programs. This also removes the danger of accidentally loading a worm or virus on your own hard disk if you lend the data medium to someone, and get it back with "dangerous cargo." **(Source: Access Control & Security Systems)**

